

DIALOG(R)File 351:Derwent WPI
(c) 2002 Derwent Info Ltd. All rts. reserv.

011179395 **Image available**

WPI Acc No: 1997-157320/199715

XRPX Acc No: N97-129854

Verification server for authentication of network user - receives authentication data from application client relayed from application server, searches for stored valid user authentication data and compares with relayed authentication data

Patent Assignee: CADIX INC (CADI-N); CADIX KK (CADI-N); CADIX KK (KYAT-N)

Inventor: TABUKI T

Number of Countries: 007 Number of Patents: 008

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 762261	A2	19970312	EP 96306390	A	19960902	199715 B
JP 9081518	A	19970328	JP 95231159	A	19950908	199723
JP 9081519	A	19970328	JP 95231160	A	19950908	199723
JP 9081520	A	19970328	JP 95231161	A	19950908	199723
US 5706427	A	19980106	US 96671241	A	19960627	199808
US 5841970	A	19981124	US 96671240	A	19960627	199903
SG 65643	A1	19990622	SG 97690	A	19970307	199935 N
US 5987232	A	19991116	US 96671242	A	19960627	200001
			US 97925634	A	19970909	

Priority Applications (No Type Date): JP 95231161 A 19950908; JP 95231159 A 19950908; JP 95231160 A 19950908; SG 97690 A 19970307

Cited Patents: -SR.Pub

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 762261	A2	E	14	G06F-001/00	
Designated States (Regional): DE FR GB IT					
US 5987232	A			G06F-011/00	Cont of application US 96671242
JP 9081518	A		9	G06F-015/00	
JP 9081519	A		9	G06F-015/00	
JP 9081520	A		10	G06F-015/00	
US 5706427	A		12	G06F-017/00	
US 5841970	A			G06F-011/00	
SG 65643	A1			H04L-009/32	

Abstract (Basic): EP 762261 A

The server verifies the authentication of users on networks. Authentication data is sent from the application client (20) and is relayed to a verification server (30) by the application server (10).

The verification server maintains a database of valid authentication data, against which it verifies received authentication data. Verification results are sent to the application server, which then processes users on the basis of these results.

ADVANTAGE - Verification server is used by number of application servers which allows for more efficient use of resources on network.

Dwg.1/6

Abstract (Equivalent): US 5706427 A

The server verifies the authentication of users on networks. Authentication data is sent from the application client (20) and is relayed to a verification server (30) by the application server (10).

The verification server maintains a database of valid authentication data, against which it verifies received authentication data. Verification results are sent to the application server, which then processes users on the basis of these results.

ADVANTAGE - Verification server is used by number of application servers which allows for more efficient use of resources on network.

Dwg.6/6

Title Terms: VERIFICATION; SERVE; AUTHENTICITY; NETWORK; USER; RECEIVE; AUTHENTICITY; DATA; APPLY; CLIENT; RELAY; APPLY; SERVE; SEARCH; STORAGE; VALID; USER; AUTHENTICITY; DATA; COMPARE; RELAY; AUTHENTICITY; DATA

Derwent Class: T01

International Patent Class (Main): G06F-001/00; G06F-011/00; G06F-015/00;

G06F-017/00; H04L-009/32

File Segment: EPI

Manual Codes (EPI/S-X): T01-H07C5A

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-81519

(43) 公開日 平成9年(1997)3月28日

(51) Int. Cl.⁵

G 0 6 F 15/00

識別記号

3 3 0

庁内整理番号

F I

G 0 6 F 15/00

技術表示箇所

3 3 0 B

審査請求 未請求 請求項の数 2 O L (全 9 頁)

(21) 出願番号

特願平7-231160

(22) 出願日

平成7年(1995)9月8日

(71) 出願人 591210910

株式会社キャディックス

東京都世田谷区新町2丁目26番15号

(72) 発明者 田次 隆明

東京都世田谷区新町2丁目26番15号 株式会社キャディックス内

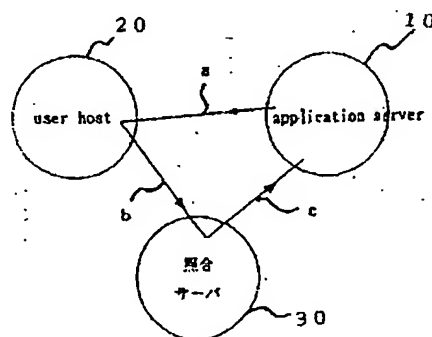
(74) 代理人 弁理士 吉田 研二 (外2名)

(54) 【発明の名称】 ネットワーク上の認証方法

(57) 【要約】

【課題】 ネットワーク上で利用者の認証を容易に行う方法を実現する。

【解決手段】 ユーザホスト20に対し、アプリケーションサーバ10は、認証データを照合サーバ30に送出するよう要求する。照合サーバ30は、「正しい」認証データを予めデータベースに保持しており、ユーザホスト20から送出されてきた認証データと、「正しい」認証データとを比較照合する。そして、この照合の結果がアプリケーションサーバ10に送出される。アプリケーションサーバ10はこの結果に基づき、利用者に認証を与える。この結果、アプリケーションサーバ10の構成が簡易化される。照合サーバ30は、複数のアプリケーションサーバ10から利用することができ、ネットワーク上の資源の運用の効率化を図ることができる。



【特許請求の範囲】

【請求項1】 ネットワーク上のアプリケーションサーバが、そのアプリケーションの利用者の認証を行う認証方法において、

前記アプリケーションサーバが、前記利用者に対し、認証データを照合サーバに送信するよう要求する認証データ要求工程と、

前記利用者が、前記認証データ要求工程におけるアプリケーションサーバの要求に対して、前記利用者の認証データを、前記利用者の識別データと共に、照合サーバに送出する送出工程と、

前記照合サーバが、前記送出されてきた認証データが、前記送出されてきた識別データの利用者の認証データであるか否かを照合する照合工程と、

前記照合サーバが、照合結果を前記アプリケーションサーバに返送する照合結果返送工程と、

前記照合結果返送工程において返送された照合結果に基づいて、前記アプリケーションサーバが前記利用者が正当な利用者であるか否かを認証する認証工程と、を含むことを特徴とするネットワーク上の認証方法。

【請求項2】 ネットワーク上のアプリケーションサーバが、そのアプリケーションの利用者の認証を行う認証方法において、

前記アプリケーションサーバが、前記利用者に対し、認証データを照合サーバに送信するよう要求する認証データ要求工程と、

前記アプリケーションサーバが、照合サーバに対し、前記利用者の識別データを送信して、前記利用者の正しい認証データを予め呼び出しておくよう要求する照合準備要求工程と、

前記利用者が、前記認証データ要求工程におけるアプリケーションサーバの要求に対して、前記利用者の認証データを、前記利用者の識別データと共に、照合サーバに送出する送出工程と、

前記照合サーバが、前記送出されてきた認証データが、前記送出されてきた識別データの利用者の認証データであるか否かを照合する照合工程と、

前記照合サーバが、照合結果を前記アプリケーションサーバに返送する照合結果返送工程と、

前記照合結果返送工程において返送された照合結果に基づいて、前記アプリケーションサーバが前記利用者が正当な利用者であるか否かを認証する認証工程と、を含むことを特徴とするネットワーク上の認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、アプリケーション利用者の認証を行う方法に関する。特に、ネットワーク上における利用者の認証に関する。

【0002】

【従来の技術】銀行などのサービス業では、取引に際し

て、相手が本人であるか否かを確認すること、すなわち認証は極めて重要な問題である。これは、他人が本人になりすまして口座からお金を引き出してしまったり、お金を振り込んでしまったりすることを防止するためである。

【0003】この認証のためには、古典的には例えば、運転免許証や、一定の身分証明書等を提出してもらい、本人であるか否かを確認している。近年、現金自動引き出し器等の発達により、磁気カードやパスワードなどによって、本人の認証を行う方法が広く採用されている。

【0004】このような「認証」は、銀行以外でも必要とされる場合は多い。例えば、研究機関などにおいては、秘密漏洩を防止すべく、一定の区域へは許可された者のみ入場を許し、それ以外の者に対しては入場を制限する場合が多い。また、会員制クラブ等でも会員であることを何らかの方法で確認しなければならない。この研究機関や会員制クラブにおいても、上記磁気カードやパスワード、若しくは会員証等を用いることも好適である。

しかし、磁気カードや会員証は紛失してしまう可能性があるし、また、パスワードも忘れてしまう可能性も決して小さくはない。そのため、本人を確認する方法として、指紋や、網膜パターン等のいわゆるバイオメトリックな物理量を認証のためのデータ（以下、認証データという）として用いる方法も提案されている。

【0005】企業内の電子ドキュメント承認プロセスでは、署名を用いて本人であることを確認し、承認することが自然である。また近年、企業ではCADの利用が一般化しており、その承認のプロセスでは署名データの形状をイメージデータとしてCADデータにはりつけることもできる。

【0006】

【発明が解決しようとする課題】近年、ネットワークの発達により、このネットワーク上で種々のサービスの提供が行われるようになった。例えば、いわゆるインターネットにおいては、WWW (World Wide Web) 等によるマルチメディアタイトルの提供サービスが広く行われている。このようなサービスの提供においては、一般の銀行等におけるサービスと同様に、一定の資格者のみアクセスを認める場合もある。このようなネットワーク上のサービスにおいても、従来のサービスと同様に、「認証」はきわめて重要な問題である。

【0007】しかしながら、ネットワーク上で本人であるか否かの認証をする場合に、上述したバイオメトリックな認証データを用いることは一般にきわめて困難である。例えば網膜パターンや指紋、あるいは掌紋等を入力する装置を各端末に備える必要があり、また、このような物理量をネットワークを介して伝送するための仕組みも新たに必要となってしまう。

【0008】そのため、ネットワーク上で用いられるバイオメトリックな物理量として、署名データを用いるこ

とが注目されている。この署名データは、いわゆるタブレットにより容易に入力することができ、かつ平面の2次元データだけではなく、署名を書くスピードや筆圧の変化もデータとしているため、本人であるか否かを認証するための認証データとして優れた特性を有している。更に、タブレットは一般に安価に構成できるので、端末のコストも安く抑えることができるという特徴を有している。

【0009】以上述べたように、パスワードなどの認証データの他、署名データ等のバイOMETリックな認証データがネットワーク上における「認証」に利用されている。

【0010】ところが、ネットワークの拡大にともない、サービスの提供者であるアプリケーションサーバの種類が増え、かつそのサービスの提供を受けるクライアントの数もきわめて膨大なものとなっている。そのため、各アプリケーションサーバがそれぞれ別個に認証を行う際の負担が過大になってきている。特に、インターネットのように世界規模で広がっている場合には、アプリケーションサーバとそのサービスの提供を受けるクライアントとの間がきわめて遠距離となる場合も多い。このような場合に、認証データのやりとりをすることがネットワーク上のトラフィックの増大に結びついてしまうことも考えられる。

【0011】本発明は、このような課題を解決するためになされたものであり、その目的は、ネットワーク上のクライアントの認証のための照合の機能をアプリケーションサーバと独立してネットワーク上に設けることによって、アプリケーションサーバの負荷を減少させるとともに、クライアントの認証を容易に行うことが可能な認証方法を提供することである。

【0012】

【課題を解決するための手段】第1の本発明は、上記課題を解決するために、ネットワーク上のアプリケーションサーバが、そのアプリケーションの利用者の認証を行う認証方法において、前記アプリケーションサーバが、前記利用者に対し、認証データを照合サーバに送信するよう要求する認証データ要求工程と、前記利用者が、前記認証データ要求工程におけるアプリケーションサーバの要求に対して、前記利用者の認証データを、前記利用者の識別データと共に、照合サーバに送出する送出工程と、をまず含んでいる。

【0013】このように、本発明は、アプリケーションサーバが認証データを外部の照合サーバに送出し、照合の手続きを外部に委託している点に特徴がある。外部に照合の手続きを委託することにより、アプリケーションサーバ自体は照合のためのデータベースを備える必要がなくなる。

【0014】そして、第1の発明は、前記照合サーバが、前記送出されてきた認証データが、前記送出されて

きた識別データの利用者の認証データであるか否かを照合する照合工程と、前記照合サーバが、照合結果を前記アプリケーションサーバに返送する照合結果返送工程と、前記照合結果返送工程において返送された照合結果に基づいて、前記アプリケーションサーバが前記利用者が正当な利用者であるか否かを認証する認証工程と、を含むことを特徴とするネットワーク上の認証方法である。

【0015】このような構成によって、本発明によれば、アプリケーションサーバ自体が認証データを保持する必要がなく、且つ、認証に必要な「照合」という手続きを照合サーバに集中して担わせることが可能である。

【0016】次に、第2の本発明は、ネットワーク上のアプリケーションサーバが、そのアプリケーションの利用者の認証を行う認証方法において、前記アプリケーションサーバが、前記利用者に対し、認証データを照合サーバに送信するよう要求する認証データ要求工程と、前記アプリケーションサーバが、照合サーバに対し、前記利用者の識別データを送信して、前記利用者の正しい認証データを予め呼び出しておくよう要求する照合準備要求工程、をまず備えている。

【0017】すなわち、照合すべき認証データがまだ得られていない時点において、あらかじめ利用者が誰であるのかを照合サーバに伝えることにより、照合サーバは「正しい」認証データを予め記憶手段から読み出しておくことができるのである。これによって、照合対象である認証データが、その照合サーバに送られてきた時に迅速に、「照合」動作を行うことができる。

【0018】そのため、第2の本発明は、上に述べた工程の他は、第1の本発明と同様の以下の工程を含むものである。

【0019】すなわち、第2の本発明は、上記工程に加えて、前記利用者が、前記認証データ要求工程におけるアプリケーションサーバの要求に対して、前記利用者の認証データを、前記利用者の識別データと共に、照合サーバに送出する送出工程と、前記照合サーバが、前記送出されてきた認証データが、前記送出されてきた識別データの利用者の認証データであるか否かを照合する照合工程と、前記照合サーバが、照合結果を前記アプリケーションサーバに返送する照合結果返送工程と、前記照合結果返送工程において返送された照合結果に基づいて、前記アプリケーションサーバが前記利用者が正当な利用者であるか否かを認証する認証工程と、を含むことを特徴とするネットワーク上の認証方法である。

【0020】このような構成によって、第2の本発明は、迅速な認証が行える認証方法である。

【0021】

【発明の実施の形態】以下、本発明の好適な実施の形態を、図面に基づいて説明する。

【0022】図1には、本実施の形態において、ネット

ワーク上に設けられているアプリケーションサーバ (Application Server) 10のサービスを利用するユーザホスト (User Host) 20と、ユーザホスト20の認証の際に利用される照合サーバ (Verification Server) 30とがネットワーク上に配置されている様子が示されている。

【0023】本実施の形態において特徴的なことは、ユーザホスト20の認証の際の照合動作が、アプリケーションサーバ10において行われるのではなく、アプリケーションサーバ10とは別体にネットワーク上に設けられている照合サーバ30を用いて行われていることである。このように、照合動作を行う照合サーバ30をアプリケーションサーバ10と独立にネットワーク上に設けることにより、個々のアプリケーションサーバ10はユーザホスト20の認証のための「正しい」認証データを保持したり、照合のための機能を有する必要がなくなる。また、図1においてはアプリケーションサーバ10としてひとつの構成しか示されていないが、ネットワーク上に複数のアプリケーションサーバ10を設けることも好適であり、この場合にはその複数のアプリケーションサーバ10から1個の照合サーバ30を利用して「照合」動作を委託することができ、複数のアプリケーションサーバ10において従来重複して備えられていた認証データの照合機能を一つにまとめることができ、効率的な資源の運用が可能となる。

【0024】また、この照合サーバ30は、ネットワーク上に複数個設けることも好適である。そして、各アプリケーションサーバ10は、認証の内容に応じて、好適な照合サーバを利用することが可能となる。例えば、認証データとして署名データが用いられる場合と、認証データとして指紋データが用いられる場合とにおいて利用する照合サーバ30を変えることも考えられる。もしくは、各利用者が自分の認証データを保持している照合サーバ30を自ら指定することも考えられよう。

【0025】図1に示されているように、照合サーバ30をアプリケーションサーバ10と独立にネットワーク上に設けることにより、認証の際のメッセージのやりとりは例えば図1において矢印で示されるようになる。図1に示されているように、まず、アプリケーションサーバ10がユーザホスト20に対して、認証データを照合サーバ30に送るように要求する(図1においてaで示される)。この認証データは、古典的にはパスワードや会員番号を利用することもできるが、バイオメトリックな物理量、例えば署名データ等を用いることが好適である。特に、上述したように、署名データは、ユーザホスト20に安価なタブレットを準備するだけで容易に入力することが可能である。

【0026】ユーザホスト20は、aの要求に対して利用者の署名データをタブレットから入力し、利用者の識

別データ(例えば会員番号や利用者名)と共に照合サーバ30にこの署名データを送出する(図1においてbで示される)。アプリケーションサーバ10は、ユーザホスト20が正しい利用者であるか否かを判断するわけであるが、その認証の際に必要な「照合」作用を外部の照合サーバ30にいわば委託しているのである。このため、照合サーバ30は、ユーザホスト20から送出されてきた認証データと識別データを予め記憶しておいて「正当な」認証データと照合する。具体的には、照合サーバ30はユーザホスト20が本人であると主張する利用者名と、その利用者の正しい認証データとをデータベースとして内部に保持している。そして、このデータベースを検索することにより、ユーザホスト20が本人であると主張する利用者についての正しい認証データ(本実施の形態においては例えば署名データ)を取り出す。そして、この取り出された認証データとユーザホスト20から送られてきた認証データとを比較・照合し、その結果をアプリケーションサーバ10に送出する(図1においてcで示されている)。アプリケーションサーバ10は、この照合サーバ30から返送されてきた照合結果に基づいてユーザホスト20に対して認証を行うのである。

【0027】本実施の形態においては、このように照合の動作を行う部分を、アプリケーションサーバ10と独立にネットワーク上に設けたので、複数のアプリケーションサーバ10に共通に重複して設けられていた照合機能を節約することができるとともに、認証動作の確実さを担保することが可能である。

【0028】なお、アプリケーションサーバ10としては、インターネット上における例えばWWWサーバや、各種のデータベース等、種々のサービスを提供するサーバが考えられる。

【0029】図2には、図1に示されているユーザホスト20やアプリケーションサーバ10及び照合サーバ30の詳細な構成を表す構成ブロック図が示されている。図2に示されているように、ユーザホスト20は、パーソナルコンピュータ等の端末から構成されており、インターネットに接続し、WWWサーバ42に接続するためのWWWブラウザのひとつであるネットスケープ(Netscape)52を備えている。なお、本実施の形態ではネットスケープ52が用いられているが、これはモザイク(Mosaic)等、他のWWWブラウザでもかまわない。ユーザホスト20はこのネットスケープ52の他に、利用者が署名データを入力するためのタブレット(Tablet)54を備えている。また、このタブレット54を制御し、署名データを取り出すためのタブレットドライバプログラム56が備えられている。このタブレットドライバプログラム56は、アプリケーションサーバ10から認証データを送出するように要求が来た場合に、その要求をネットスケープ52を介して受け

取り、タブレット54を駆動して得られた認証データ（署名データ）を、照合サーバ30に送出する。なお、図1に示されているメッセージのやりとりa、b、cと同一のメッセージのやりとりに対して同一の符号a、b、cが図2にも付されている。

【0030】アプリケーションサーバ10は、Unixマシン上に構築される場合が多い。このアプリケーションサーバ10には、図2に示されているようにマルチメディアタイトルを提供するWWWサーバ42と、利用者の正当性を確認するための署名照合要求プログラム44とが備えられている。照合サーバ30は、アプリケーションサーバ10と同様にUnix等のマシン上に構築されており、正当な利用者とその利用者の認証データとを登録した登録データ62を有している。そして、上記ユーザホスト20から送出されてくる利用者名（利用者の識別コード）にもとづいて、ユーザホスト20から送出されてきた認証データ（本実施の形態においては署名データ）と予め登録されている「正しい」認証データを照合し、照合結果をアプリケーションサーバ10の署名照合要求プログラム44に送出するのである。

【0031】照合サーバ30の登録データ62は、本実施の形態においては、リレーショナルデータベース（以下、RDBという）によって管理されている。この登録データのRDB内の様子が図3に示されている。図3に示されているように、登録データは各正当な利用者毎に所定のデータを記録した表の形で記録されている。図3に示されているように、まずフラグ（flag）は、システムの種々の状態を表すためのフラグであり、例えば削除フラグ（その利用者がシステムから削除されたか否かを表す）等として用いられる。また、システムユニークキー（SysUniq Key）は、各利用者に与えられるシステムキーであり、照合サーバ30におけるテーブル（図3に示されている）の中で唯一に定められる。また、登録タブレットタイプは、その利用者が利用するタブレットのタイプを表す。また、署名データ（Signature data）は、タブレット54上で動く電子ペンの動きを表す時系列データである。この署名データには、二次元的な位置を表す情報だけではなく、筆圧やペンの速度も含まれているため、本人であるか否かの認証を精度よく行うことが可能である。

【0032】このように、照合サーバ30内部のRDBには、システムユニークキーと、署名データとが登録されているため、ユーザホスト20から送出された署名データ及び利用者を表すシステムユニークキーを用いて、この送られてきた署名データが正当なものであるか否かを判断することが可能である。この判断の結果の内容については後で説明する。

【0033】本実施の形態におけるRDBにおいてはシステムユニークキーと署名データの他に、システム要求項目（System required items）

と呼ばれる登録項目が記憶されている。図3に示されているように、システム要求項目としては、利用者の名前（Name）、利用者の誕生日（Date of birth）及び利用者の電話番号（Phone #）が登録されている。これらのシステム要求項目は、システムユニークキーの代わりに用いられるものである。すなわち、システムユニークキーは後述するようにアプリケーションサーバ10と照合サーバ30とが保持しているキーであり、利用者を識別するためのキーであるが、利用者は自分に与えられたシステムユニークキーを必ずしも覚えていないとは限らない。そのため、利用者が登録されている署名データを確認したい場合等において、システムユニークキー以外で利用者を特定できる手段が存在した方が望ましい。このような場合にシステムユニークキー以外でも、利用者の名前や誕生日、そして電話番号等で利用者を識別し得るようにしたのである。

【0034】更に、本実施の形態においては、図3に示されているように、オプションフィールド（Optional fields）が設けられている。このオプションフィールドに登録されているデータはいわゆるシステム監査用のデータであり、照合サーバ30のシステムの管理者が照合サーバ30の動作等を管理する際に用いられる管理データである。図3に示されているように、この管理用のデータとしては、データの作成日（Creation date）、データの作成者（Creation host）、また、最終アクセス日（Last acc. date）や、最終アクセス者（Last acc. by）、その他アクセス回数（access count）や照合が失敗した回数（failure count）等、種々のデータを保持することが可能である。

【0035】また、アプリケーションサーバ10にも照合サーバ内のRDBに対応して、利用者についての情報を登録したRDBが備えられている。このアプリケーションサーバ10内のRDBに登録されている内容が図4に示されている。図4に示されているように、各種の登録データが個々の利用者毎に登録されている。図4に示されているように、まず、「照合サーバ名」は、その利用者が送ってきた認証データ（署名データ）がどの照合サーバ30によって照合されるべきか否かを表すものである。図1に示された構成図においては、照合サーバ30はひとつしか示していなかったが、ネットワーク内に複数の照合サーバ30が存在することも構成として可能である。例えば、各利用者は、自分が連絡を取りやすい照合サーバ30を使用したいと思う場合もあるであろうし、またアプリケーションサーバ10が各利用者毎に照合サーバ30を管理上の理由により変更したいと考える場合もあるであろう。

【0036】図4に示されているフラグ（flag）とシステムユニークキー（Sys Uniq Key）と

は、図3におけるフラグ及びシステムユニークキーと同一のものである。このシステムユニークキーは、上述したように、照合サーバ30のRDBの中で唯一に定められているものである。換言すれば、照合サーバ30が異なる利用者については、同一のシステムユニークキーが割り当てられる可能性も存在する。したがって、利用者の識別は、厳密には、このシステムユニークキーと照合サーバ名とを組み合わせることにより行われることになる。アプリケーションユーザキー (App. user key) は、そのアプリケーションサーバ10の提供するサービスを受けられるか否かを表すキーである。場合によっては図4に示されているように追加アプリケーションユーザキー (Additional app. user key) が設定される場合もある。更に、図4に示されているように作成日 (Creation date) や最終アクセス日 (Last acc. date)、最終アクセス者 (Last acc. by)、アクセス回数 (access count)、照合が失敗した回数 (failure count) 等が図3に示されている照合サーバ30内のRDBに対応して登録されている。また、具体的な項目名は示されていないが、アプリケーションオプションフィールド (Application optional fields) にアプリケーションが利用する所定の登録データを登録することも好適である。

【0037】図5には、本実施の形態に係る照合サーバ30がサポートするプロトコルの説明図が示されている。図5に示されているように、まずプロトコル「キーの登録」においては、アプリケーションサーバ10が所定の必須項目を含むメッセージを照合サーバ30に送出する。照合サーバはこれらの必須項目をRDBに登録すると共に、システムユニークキーを生成する。このシステムユニークキーはRDBに登録されると共に、アプリケーションサーバ10に返送される。このようにして、利用者を識別するシステムユニークキーが照合サーバ30において生成される。このシステムユニークキーはアプリケーションサーバ10においてもRDB内に登録され、照合サーバ30とアプリケーションサーバ10との間でシステムユニークキーの共有がなされる。

【0038】次に、プロトコル「署名データの登録」においては、アプリケーションサーバ10が、システムユニークキー、3個の署名データ、タブレットタイプ等を、照合サーバ30に送出し、「正しい」署名データを照合サーバ30内のRDBに登録させる。ここで、3個の署名データを送出するのは平均的な署名データの値を照合サーバにおいて求めて、平均的な値をRDB内に登録するためである。登録が正常に完了すれば、戻り値「ok」をアプリケーションサーバ10に返送し、既に登録が行われている場合等には「error」を戻り値として返送する。また、3個の署名データが互いに著し

く異なりすぎている場合には、署名データとしての信頼性が低いため、登録は行わずに「unstable」を戻り値として返送する。

【0039】プロトコル「照合準備」においては、アプリケーションサーバ10が、システムユニークキーのみを照合サーバ30に送出し、「正しい」認証データをRDBからキャッシュに呼び出させておく。このように、実際の認証データとの照合プロトコルに先立って、認証データを予め呼び出させておくことにより、後述するように迅速な照合処理が行えるのである。本プロトコルは、処理の迅速化のために行われるのであり、迅速化が必要でない場合には、本プロトコルを省略し、直接、後述する「照合」プロトコルを発行してもよい。尚、「正しい」認証データの呼び出しが正常に完了した場合にはメッセージIDがアプリケーションサーバ10に返送されるが、エラーが生じた場合には「error」を戻り値としてアプリケーションサーバ10に返送する。

【0040】プロトコル「照合」は、ユーザホスト20がシステムユニークキー、署名データ、タブレットタイプ、及びメッセージIDを照合サーバ30に送出し、照合動作を行わせるプロトコルである。尚、メッセージIDは、先に「照合準備」プロトコルが発行されている場合にその戻り値として返送されたメッセージIDが用いられる。尚、後述するように、照合結果はアプリケーションサーバ10に送出されるが、その際、このメッセージIDはどの利用者の認証であるかを識別するタグとして使用される。すなわち、本実施の形態においては、このメッセージIDは、認証の識別用の番号であると共に、キャッシュに認証データが既に呼び出されていることをも表すIDでもある。この場合メッセージIDの最初の作成は照合サーバ30が行い、照合準備要求に対する応答の時にメッセージに付与されるのである。

【0041】一方、もし「照合準備」プロトコルが発行されていない場合には、このメッセージIDは、単にどの利用者に対する認証であるのかを識別する識別子としての役割しか果たさない。この場合はメッセージIDの最初の作成はアプリケーションサーバ20である。

【0042】さて、照合サーバ30は、このメッセージIDが自己が付与したものか否かによって、認証データが既にキャッシュに読み出されているか否かを否かを知ることができる。既に「正しい」認証データが呼び出されている場合には、そのデータと、送られてきた認証データとを比較・照合する。「正しい」認証データが呼び出されていない場合には、RDBから新たに「正しい」認証データが呼び出されて、比較・照合動作が行われる。

【0043】比較・照合の結果、両者が非常に近く正しい認証データであると判断される場合には、戻り値として「yes」がアプリケーションサーバ10に送出される。一方、送られてきた認証データが「正しい」認証デ

ータと全く異なったものである場合には戻り値として「no」が送出される。比較・照合の結果、正しい認証データであるか否かが不明な場合は、戻り値として「maybe」をアプリケーションサーバ10に送出する。不明な場合の対処は、各アプリケーションサーバ10ごとに異なるであろうが、例えば、署名を利用者にやり直させる等の処置が執られることになろう。また、比較・照合をする「正しい」認証データが見つからなかった場合等においては、戻り値として「error」がアプリケーションサーバ10に送出される。

【0044】次に、実際の利用者の認証が行われる様子を図6に基づいて説明する。以下、この利用者のことをアプリケーションクライアントと称する(図6)まず、アプリケーションクライアントは、ユーザホスト20を介してアプリケーションサーバ10に対して、接続要求を行う。

【0045】これに応答してアプリケーションサーバ10は、アプリケーションクライアントに対して、アプリケーションキーの入力を要求する。これに応答して、ユーザホスト20の表示装置上にはアプリケーションキーの入力を促すプロンプトが表示される。

【0046】アプリケーションクライアントがユーザホスト20において所定のキーを入力すると、そのデータがアプリケーションサーバ10に送出される。

【0047】アプリケーションサーバ10は、このキーデータを受信すると、署名データの照合準備の要求を照合サーバ30に送出する。この照合準備要求は、上述したように処理の迅速化のために行うものであり、省略することも可能である。

【0048】照合サーバ30は照合準備要求を受信すると、上述したように、認証データをRDBから読み出し、キャッシュに記憶させると共にアプリケーションサーバ10に対してメッセージID、暗号キーを送出する。暗号キーは通信データの暗号化に用いられるキーであり、暗号化が必要なければ送らなくともよい。

【0049】上記メッセージID等を受信したアプリケーションサーバ10は、アプリケーションクライアントに署名を入力させるため、署名入力要求を出力する。

【0050】この署名入力要求に応じてユーザホスト20においては署名入力プログラムが起動する。このプログラムの起動に基づき、アプリケーションクライアントはユーザホスト20に備えられているタブレット54を用いて署名を行う。ユーザホスト20は、タブレット54から入力された署名データを認証サーバ30に送出する(照合要求)。この際、図6に示されているように、キーデータや、メッセージIDが署名データとともに、照合サーバ30に送出される。

【0051】照合サーバ30は、照合要求に基づき、照合を行い、その結果をアプリケーションサーバ10に返送する。照合サーバ30は、照合要求の際に同時に送られてきたメッセージID等に基づいて、照合結果を送出すべきアプリケーションサーバ10を特定することができる。

【0052】アプリケーションサーバ10は照合結果に基づき、認証を行う。このときの動作は各アプリケーションサーバ10により異なるが、照合結果がYESの場合には「認証」を与えることになり、それ以外の場合には「認証」を与えない、若しくは署名をやり直させることになろう。

【0053】以上述べたように、本実施の形態によれば、認証の際に行われる照合動作を外部の照合サーバに委託したので、アプリケーションサーバの負荷を減らすと共に照合動作の簡明化を図ることができる。

【0054】

【発明の効果】以上述べたように、第1の本発明によれば、ネットワーク上における利用者の認証をアプリケーションサーバ以外の照合サーバに行わせたので、アプリケーションサーバの構成が簡単になり、また、複数のアプリケーションサーバが同一の照合サーバを利用することで、ネットワーク上の資源をより効率的に利用することができるという効果を奏する。

【0055】また、第2の本発明によれば、照合に先立って、照合準備要求工程で、認証データを予め呼び出させておいたので、迅速な照合を行うことが可能である。

【図面の簡単な説明】

【図1】 本発明の実施の形態の構成を表す構成図である。

【図2】 本発明の実施の形態の構成の詳細を表す説明図である。

【図3】 照合サーバ内のRDBの構成を表す説明図である。

【図4】 アプリケーションサーバ内のRDBの構成を表す説明図である。

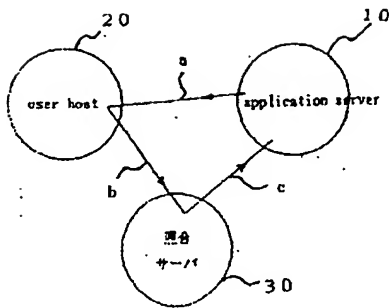
【図5】 照合サーバがサポートするプロトコルを表す説明図である。

【図6】 本実施の形態におけるメッセージの交換を表す説明図である。

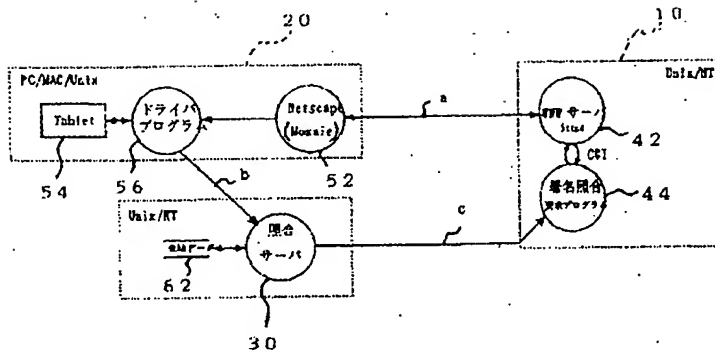
【符号の説明】

10 アプリケーションサーバ、20 ユーザホスト、30 照合サーバ、42 WWWサーバ、44 署名照合要求プログラム、52 ネットスケープ、54 タブレット、56 タブレットドライバプログラム、62 登録データ。

【図1】



【図2】



【図5】

照合サーバプロトコル

リクエストに共通なデータ: データバージョン、署名タイプ、圧縮タイプ

リクエスト	リクエストに格納したデータ項目	戻り値	説明
キーの登録	必須項目(Name, BirthDate, Phone)	System uniq key error	照合サーバにシステム必須項目を考えて、システムユニークキー(登録キー)を得る
署名データの登録	System uniq key, 署名データ x3 タブレットタイプ	ok/error: Unatable	登録キーと共に登録の登録用署名データを送付し、署名の登録をする
照合	System uniq key, 署名データ、 タブレットタイプ メッセージID	Yes No maybe error	登録キーとともに照合される署名データを返却して照合要求をする 照合が正常な結果であればメッセージIDを付ける
照合準備	System uniq key	error メッセージID、署名	照合に先立って登録キーとともに署名データの読みだし要求をする。 照合されるメッセージIDを使い照合することもできる

【図3】

			flag
			Sys Uniq Key
			登録タブレットタイプ
			Signature data
			Name
			Date of birth
			Phone #
			Creation date
			Creation host
			Last acc. date
			Last acc. by
			Access count
			failure count

System required items

Optional fields

[illegible]

The diagram illustrates the flow of an application process between an **アプリケーションクライアント** (Application Client) and an **アプリケーションサーバ** (Application Server).

Client Side (Left):

- 接続要求** (Connection Request): The initial step from the client to the server.
- アプリケーションキー入力プロシージャ** (Application Key Input Procedure): The process for entering the application key.
- キー送信** (Key Transmission): The transmission of the application key to the server.
- 署名入力プログラム起動** (Signature Input Program Activation): The activation of the program for entering a signature.
- 署名データの送信** (Signature Data Transmission): The transmission of the signature data to the server.
- 結果に依存したアクション** (Action Dependent on Result): The final action taken based on the server's response.

Server Side (Right):

- 接続要求受信** (Connection Request Reception): Reception of the connection request from the client.
- アプリケーションキー入力要求** (Application Key Input Request): The request for the application key from the client.
- キー受信** (Key Reception): Reception of the application key from the client.
- 署名入力要求** (Signature Input Request): The request for the signature from the client.
- 署名データ受信** (Signature Data Reception): Reception of the signature data from the client.
- 照合結果送信** (Matching Result Transmission): The transmission of the matching result back to the client.

Intermediate/Shared Elements:

- 照合準備要求** (Matching Preparation Request): A request from the client to the server for preparation.
- 照合準備要求受信** (Matching Preparation Request Reception): Reception of the preparation request from the client.
- マッチングID、暗号キー** (Matching ID, Encryption Key): Data received from the server, used for matching and encryption.
- マッチングID、暗号キー** (Matching ID, Encryption Key): Data sent from the client to the server for matching and encryption.
- マッチングID、暗号キー** (Matching ID, Encryption Key): Data received from the server, used for matching and encryption.